UNITED STATES DISTRICT COURT
District of New Jersey

RECEIVED-CLERK
U.S. DISTRICT COURT
2007 JAN [illegible] P 12: [illegible]

HAROLD C. "HAL" TURNER v. 4CHAN.ORG et al Doc. 2

Harold C. "Hal" Turner D/B/A Turner Radio Network D/B/A Hal Turner Radio Show Plaintiff,	:	Hon. Civil Action No. 07cv306(PGS)
v.	:	**DECLARATION OF HAROLD C. "HAL" TURNER IN SUPPORT OF PLAINTIFF'S ORDER TO SHOW CAUSE, APPLICATION FOR TEMPORARY RESTRAINING ORDER AND MOTION FOR PRELIMINARY INJUNCTION**
4Chan.org 7chan.org Ebaumsworld.com NexisOnline.net Abjects.com John Doe(s) 1-1000 Defendants:	:	

I, HAROLD C. "HAL" TURNER, hereby declare and say:

1. I am the owner and sole proprietor of TURNER RADIO NETWORK and Host of "THE HAL TURNER RADIO SHOW."

2. This Declaration is based upon personal knowledge except where stated to be on information and belief, in which case I believe such statements to be true.

3. I respectfully submit this Declaration in support of my (Plaintiff's) request for an Order to Show Cause, application for temporary restraining order and motion for preliminary injunction, pursuant to Rule 65 of the Fed. R. Civ. P., seeking to enjoin the Defendants during the pendency of this action from allowing users of their Internet Services to conspire, organize, incite and teach others how to unlawfully electronically attack my internet web sites making them unavailable to the

Dockets.Justia.com

public; Defrauding me through intentional and malicious use of automated computer software designed to intentionally receive the content of my web sites over and over again - sometimes tens of thousands of times per day - to the same computers, for the expressed purpose of increasing the data flow into and out of my web sites, with the intent to cause me increased data flow costs so as to wreck me financially; violating my Copyright by unlawfully redistributing copies of my weekly talk-radio show; Committing Mail Fraud and Wire Fraud by placing false orders for goods and services to be shipped to and billed to me; Committing telephone harassment of my radio show, my personal private home telephone and the home telephone of my 62 year old mother who lives in Tunkhannock, PA; Committing Extortion by demanding I shut down my web sites and radio show under threat of continuing all the activities above.

4. While it is being broadcast live on the Internet "The Hal Turner Radio Show" (hereafter referred to as "The Show") is the single, most-listened-to talk radio program in the entire world on the America Online (AOL)/SHOUTcast internet streaming audio system. While it airs, The Show has more listeners on the internet than radio station WNYC AM 820, in New York City; more

listeners on the Internet than radio station WBUR 90.9 FM in Boston, MA; and is growing in popularity and listenership. The reasons The Show is so popular has to do with unfettered free speech afforded to callers and exercised by myself as Host. People can call-in and use any language or terminology they choose, to express their thoughts or feelings about social, political, cultural, racial or religious issues, without fear of being censored or cut off. The Show is the literal embodiment of the First Amendment to the Constitution for The United States of America.

5. Allowing and exercising such unfettered free speech has caught the attention of a number of self-anointed arbiters of political correctness who seem to think they have a right to decide for others, what should and should not be allowed in public discourse. Such politically correct tyrants have, for the six years that the Show has aired, used every method possible to stifle, censor, smear, vilify, besmirch, disrupt, interrupt and shut down The Show. All their efforts have failed, until now.

6. At some point prior to December 20, 2006, a group of self-anointed tyrants utilized an internet relay chat (IRC) known as irc.abjects.com in a chat room called

#halturner, to concoct and implement a scheme to disrupt The Show by placing dozens of crank calls while the show aired. Since callers to The Show are not pre-screened for content, they were able to get on the air and pull their pranks, thus successfully disrupting the program for the three hours it aired.

7. After The Show ended, I decided to research the Caller ID for phone lines coming into The Show. The research allowed me to identify five or six specific telephone numbers that had repeatedly called The Show. Two days later, on December 22, 2006, I chose to publicly release those phone numbers via my web site HalTurnerShow.com as a warning to others not to engage in that type of activity anymore.

8. When I released those phone numbers, the John Doe Defendants named in this action at law - and hundreds of their John Doe cohorts from the Defendant's web sites - became enraged that I dared to fight back.

9. Later, on or about December 23, 2007, one or more of the John Does posted to the internet my personal, private, unlisted home telephone number, the private unlisted home telephone number of my 62 year old mother along with scurrilous and false accusations claiming I engaged

in Domestic Violence, Animal cruelty, use illegal drugs, and a virtual avalanche of other scurrilous and false allegations. Since I am a "public figure" as defined by the U.S. Supreme Court Case "*New York Times v. Sullivan*" I do not have a cause of action for libel.

10. Within hours of the publishing of my private unlisted home telephone number, my home telephone began to receive dozens of harassing, abusive and threatening calls. The first such call was received by my wife, Phyllis Turner. We later came to find that the John Doe Defendant caller recorded that crank call and publicly published the audio on the Internet for others to hear. This had the effect of encouraging hundreds of others to engage in the same activity. These calls continued into all hours of the day and night, continued throughout Christmas Eve and Christmas Day and became so bothersome that we had to shut off our telephone and, ultimately, change our telephone number.

11. Almost simultaneously with the calls to my home, my 62 year old mother who lives with her 70 year old husband in Tunkhannock, PA, started receiving similar calls. So determined were these John Doe Defendants to disrupt and harass, they continued to place these harassing and threatening calls throughout Christmas Eve and even on

Christmas Day. These calls became so bothersome to my mother and her husband - who is recovering from Leukemia - they too had to change their telephone number.

12. At or about 12:30 PM EST on December 23, 2006, as I do each day, I examined the real-time, graphical data-flow chart for my computer server which is co-located at a data center in Parsippany, NJ operated by Net Access Corporation. That real-time graphical data-flow chart showed that my computer server had begun to receive extraordinary amounts of internet data traffic. Data flow out of my computer server suddenly increased about 100 times the normal rate. This became very worrisome to me very quickly because I must pay for all data that flows into and out of my web site computer server. I logged-in to the administrative area of my computer server and called up a "Netstat" report to identify what connections were being made to the computer server. I found thousands of simultaneous connections from dozens of users, but these connections were strange: They were emanating from the same Internet Presence (IP) addresses. These connections to my computer server were systematically and deliberately calling for and receiving tens of thousands of exact duplicate copies of my web sites and / or exact duplicates of certain files

on those sites. These exact duplicates were all going to the exact same computers on the exact same day(s).

13. In common internet parlance, data flow into and out of a computer server is known as "bandwidth" and the type of activity described in Item #12 above, being done to my computer server, is commonly called "Bandwidth rape." It is a malicious form of data leeching activity designed specifically to suck the data out of a web site so thoroughly and for so long, that the site is financially killed by increased bandwidth costs. In legal parlance, this type of malicious activity is deliberate Common Law Fraud because it is not fair dealing; there is absolutely no possible legitimate reason for anyone to do this, ever. Once a person has a single copy of my web site content or single copy of a particular file, they have the ability to make duplicates without ever going to my computer server again.

14. Upon realizing what was happening, I began to analyze the logs of connections to my computer server using the "Netstat" command which shows all connections. Those logs helped me isolate and begin blocking the offending IP addresses. I contacted the data center where my server is located, Net Access Corporation in Parsippany,

NJ and asked them to begin blocking the worst offending IP addresses. They did. The server bandwidth started returning to normal. Apparently, the attackers realized they were being blocked out, so they publicly published messages on the one or more of the Defendants web sites, asking others to join in the attacks and providing detailed instructions about how to perpetrate the attacks. The data flow once again jumped to 100 times normal. Late in the day on December 23, or early I the morning on December 24, I decided to temporarily shut off the web sites hoping that the attackers would go away.

15. Over the Christmas holiday, I researched Bandwidth rape and learned that it can be defended against by installing a file which tells automated software that my sites will not accept their use. I installed on my computer server a file called "robots.txt" which instructs automated software that my computer server will not accept their connections. I thought the problem was solved. I was wrong.

16. On December 26, 2006 I turned the web sites back on and almost immediately attacks began anew, but in a different, more destructive form: SYN-ACK data packet floods. When one computer tries to communicate with

another computer over the Internet, the origin computer sends a "SYNCHRONIZE (SYN)" data packet to the target computer it is trying to reach. This data packet tells the target computer to prepare to communicate with the origin computer via certain internet addresses, IP's. The target computer then sets aside a small amount of its resources to be able to handle whatever the origin computer needs and sends and ACKNOWLEDGEMENT (ACK) data packet to the origin computer saying it is ready to communicate. In a SYN-ACK flood attack, the origin computers deliberately send a SYN data packet but never follow through with communication. This is a malicious act because as the target computer sets aside resources to prepare to communicate with tens of thousands of these origin SYN requests, the resources of the target computer get used up, making the computer unable to continue handling other, legitimate SYN requests. This type of activity is specifically designed to cause the target computer to be unavailable to legitimate users, who, when they try to connect, can get no reply from the targeted computer because its resources have become overloaded.

17. Since SYN-ACK data packets are absolutely essential to the proper operation of computer communication via the internet, there is absolutely no technological defense

that I am aware of, which can prevent this type of attack. As such this type of activity - designed to make data unavailable - was specifically outlawed by the Computer Fraud and Abuse Act 18 USC 1030.

18. For the purposes of this legal action, my computer server is a "protected computer" as defined in 18 USC 1030 because it is "used in interstate commerce" for the purpose of "communication." Hence, the provisions of 18 USC 1030 apply to my computer server and protect it.The attacks outlined above violate that federal law.

19. On December 28, 29 and 31, 2006, additional SYN-ACK attacks were launched against my computer, flooding it with upwards of 100 times the normal inbound data, which I have to pay for, and making it impossible for the computer server to handle legitimate communication requests. On December 31, 2006, I had to shut off my web sites again to protect myself from being Bankrupted on account of these attacks.

20. On or about Tuesday, December 26, I received an e-mail from a local Papa Johns Pizza Store advising me they were filling my internet order for about $93 in pizza and telling me the pizzas would be delivered soon. I

placed no such order. I called the store to cancel it and told them it was a case of WIRE FRAUD.

21. On or about Wednesday, December 27, I once again aired "The Hal Turner Show" which ended around 11:00 PM EST. At about 1:00 AM on Thursday, December 28, our home doorbell rang waking up me and my family. It was a Pizza delivery from a local pizza store, filling another Pizza order which I did not place. The pizza delivery man showed me his delivery slip which showed my name, address and telephone number. I placed no such order. I told them this was another case of WIRE FRAUD.

22. On or about Friday, December 29, at about 1:00 in the afternoon, our home doorbell rang again with yet another pizza delivery, this one telephoned into the pizza shop by someone fraudulently claiming to be me, but which I did not order. As before, the pizza delivery man showed me a delivery slip with my name, address and home telephone number. I placed no such order. I told them this was another case of WIRE FRAUD.

23. On or about Saturday, December 30, 2006, two large boxes were delivered to my home by the United States Postal Service. Inside were bulk amounts of shipping boxes

shipped to my home by the internet auction web site, EBAY.com. These boxes are shipping supplies which are designed to allow EBAY sellers to ship goods to EBAY buyers. I placed no such order for any such supplies. I have told EBAY this was a case of MAIL FRAUD and they told me to ship the supplies back to them.

24. Since these attacks commenced, I have received e-mails and electronic messages posted to my web site visitor comments area trying to Extort my surrender. The wording varied, but the message is the same:
"We will not stop until you shut down your web site and your radio show." This attempt to force me to do something that I am unwilling to do - surrender a lawful $60,000 per year and growing enterprise - is Extortion.

25. The attacks against my computer server are not an isolated incident of crime or some type of anomalous behavior. In October, 2006, the United States Department of Homeland Security issued a Terrorist Attack Advisory for National Football League Stadiums in many major cities because of threats to detonate truck bombs at seven of those stadiums. Those threats were published on and by a user of the web site of defendant 4chan.org.

36. Repeated efforts to contact the owners of the web sites 4chan.org and 7chan.org to put a halt to these activities have failed because their web site registrations which show owner contact information, are intentionally "Privatized" making owner information unavailable except through subpoena. Efforts to contact Defendants Ebaumsworld.com, Nexisonline.com and Abjects.com have gone unanswered.

37. Since the activities mentioned above have taken place consistently over eight weeks, I am experiencing incalculable harm with no other remedy at law. I need immediate relief through the courts in the form of Temporary Restraints and a permanent injunction. I hereby motion for such relief.

38. I respectfully request that the Court, in its discretion, waive the requirement that plaintiff file a bond on the grounds that there is no risk of harm faced by Defendants or their businesses if they are ordered to cease, temporarily, the activities and unlawful acts being organized via their web sites.

39. No prior request for the relief sought herein has been made.

costs and possibility of being thrown out of the new data center are causing incalculable harm to me.

33. On January 10 and 17, two additional Denial of Service attacks occurred against my server, both organized and promoted on the Defendant(s) web sites. The attack on the 17th, forced Net Access Corporation to once again 'null route" my server to protect their other data center customers. I was not told of this null routing by the data center.

34. On January 18, 2007, a number of regular visitors to my web site telephoned me saying they could not access my site. Upon investigation, I determined that Net Access Corporation has, in fact, null routed access to my server again to protect their other customers and as of now, I am effectively out of business because of the Denial of Service attacks.

35. As of today, January 19 2007, The Hal Turner Show and Turner Radio Network have been maliciously electronically crippled by repeated denial of service attacks being organized and promoted on the Defendant(s) web sites.

30. On or about______________ I received an email from a person purporting to be an administrator or other person in authority at the web site ebaumsworld.com. That e-mail acknowledged that their site supported the attacks launched against me, which indicates to me they were willing participants or accessories to the acts outlined in this declaration.

31. On January 3, another Denial of Service attack was launched at my server, taking The Show off the internet.

32. On January 9, 2007, I was notified in writing by my data center, Net Access Corporation, that repeated Denial of Service attacks against my server, they will not continue service to me. They had to "null route" (i.e. shut off access to) my server on January 3 to protect their other customers from the inbound attack against my server. They advised that if future inbound attacks occurred, they would be forced to immediately halt service to me so as to protect their other customers. Their letter requires I remove my server from their data center on or before February 15. While I have made arrangement for a new data center to provide service to me, the cost for such service is sixty-one percent (61%) more expensive per month at minimum, and if these Denial of Service attacks continue, the added

the next ten hours, until the data center could clear the inbound data backlog.

28. On or about Friday, January 5, 2007, a Manager from the United States Post Office at North Bergen, NJ came to my home to ask if I had ordered a truckload of postal shipping supplies. I told him no. He told me the North Bergen Post office had one or more Pallets of shipping supplies, allegedly ordered by me, but they were hesitant to deliver it because it appeared to be a fraud. I told the Postal Manager it was, in fact additional mail fraud and he told me he would alert U.S. Postal Inspectors for federal investigation.

29. On or about Friday, January 5, 2007, the owners of web site 7chan.org removed the front page of their site and put in its place an apology to me. The page showed an image of a Five Dollar Bill, with an altered photograph of me in the middle of that bill, and the caption above the bill read as follows" WE'RE SORRY WE TOOK ALL UR MONIES, HERE" as if to give me the fake five dollar bill. This act appears to be an overt acknowledgement that they deliberately attacked my web site and deliberately cost me money.

26. The attacks against my computer server are felonies under 18 USC 1030. Mail Fraud and Wire fraud are also felonies. Extortion is yet another felony. Mail Fraud, Wire Fraud and Extortion fulfill the necessary 'Predicate Felonies" in order to declare 4chan.org 7chan.org and ebaumsworld.com each, a Racketeer Influenced Corrupt Organization under Title 18, United States Code, Sections 1961-1968. I do hereby assert that 4chan.org and 7chan.org are, in fact, Racketeer Influenced Corrupt Organization(s) and, pursuant to 18 USC Section 1964(a) I request this civil action proceed, in part, under that law.

27. On January 3, 2007, during my live radio show which airs from 9:00 PM until 11:00 PM EST, my computer server suffered the largest, most disruptive attack to date. A sudden and dramatic increase of inbound traffic hit the server at six-hundred-sixty megabits per seconds (660 Mbps.) This attack was so enormous and so sustained that it saturated routers in the data center, taking my web site off line and also halting normal computer data flow for hundreds of other customers whose computers are also inside the data center. So damaging was this attack that the data center had to shut off all access to my computer server, rendering me helpless to conduct a radio show or to do business through that server for

40. For the reasons set forth in this and the accompanying papers, I respectfully request that the Court grant the relief sought herein in all respects.

I declare under penalty of perjury and pursuant to 28 U.S.C. 1746 that the foregoing is true and correct.

Dated: North Bergen, New Jersey

January 19, 2007

BY: Harold C Turner

Harold C. "Hal" Turner